

A

03/31/99

Sir:
P T O

Date: March 31, 1999

Transmitted herewith for filing is the Patent Application of:

Inventor(s): Daryl C. Cromer et al.

For: DATA PROCESSING SYSTEM AND METHOD FOR MAINTAINING SECURE DATA BLOCKS

XX 4 Sheets of Drawing(s) are enclosed.

XX	20	Pages of Specification are enclosed.
----	----	--------------------------------------

The filing fee has been calculated for other than a Small Entity:

[illegible]

XX Charge my Deposit Account No. 00-1990 in the amount of \$ 760.00

XX The Commissioner is hereby authorized to charge payments of (1) any additional filing fees required under 37 CFR 1.16, and/or (2) any patent application processing fees under 37 CFR 1.17 associated with this application or credit any overpayment to Deposit Account No. 09-1990.
A duplicate copy of this sheet is enclosed. 50-056

SEND CORRESPONDENCE TO:
IBM Corporation
PC Company Legal Dept.
Dept. 9CCA/Bldg. 002-2
P.O. Box 12195
Research Triangle Park, NC 27709

Respectfully submitted,

By: George E. Grosser
George E. Grosser
Registration No. 31,782
Phone: 919-254-4753

RP9-99-048

ic135 US PTO

09/28/2018 18:52

03/31/99

EX-105-410/113 US
I hereby certify that this paper or fee is being deposited with the
United States Postal Service Express Mail Post Office to Addressee
service under 37 CFR § 1.10 on the date indicated above and is
addressed to: ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D. C. 20231

on

Date of Deposit

Signature

**DATA PROCESSING SYSTEM AND METHOD FOR MAINTAINING SECURE
DATA BLOCKS**

Background of the Invention

1. Field of the Invention:

5 The present invention relates in general to data
processing systems and, in particular, to a data processing
system and method for maintaining secure blocks of data
within the system. Still more particularly, the present
10 invention relates to a data processing system and method for
maintaining secure blocks of data within the system by
encrypting the blocks of data utilizing a hardware master
key pair.

2. Description of the Related Art:

15 Personal computer systems are well known in the art.
They have attained widespread use for providing computer
power to many segments of today's modern society. Personal
computers (PCs) may be defined as a desktop, floor standing,
or portable microcomputer that includes a system unit having
a central processing unit (CPU) and associated volatile and
20 non-volatile memory, including random access memory (RAM)
and basic input/output system read only memory (BIOS ROM), a
system monitor, a keyboard, one or more flexible diskette
drives, a CD-ROM drive, a fixed disk storage drive (also
known as a "hard drive"), a pointing device such as a mouse,
25 and an optional network interface adapter. One of the
distinguishing characteristics of these systems is the use
of a motherboard or system planar to electrically connect
these components together. Examples of such personal

computer systems are IBM's PC 300 series, Aptiva series, and Intellistation series.

Encryption algorithms are known to ensure that only the intended recipient of a message can read and access the message. One known encryption algorithm is an asymmetric, or public key, algorithm. The public key algorithm is a method for encrypting messages sent from a first computer system to a second computer system. This algorithm provides for a key pair including a public key and a private key for each participant in a secure communication. This key pair is unique to each participant. An example of such an encryption scheme is an RSA key pair system.

With the proliferation of Internet services, a need has arisen to identify and authenticate the remote users. For example, an Internet electronic mail service requires a user's name and password prior to permitting access to the user's account. Many other Internet services also require a user's name and password prior to permitting access.

In order to provide more efficient access to these services, an Internet service may provide a block of data, commonly called a "cookie", to a client computer system which includes information typically needed by the service. The cookie includes information associated with both a particular user and the service which provided the cookie. The cookie often includes the associated user's name, and password, and may include the user's credit card information, address, preferences for using the service, and other data. Therefore, a cookie stores information associated with a particular user for a particular service.

A single user may have many cookies stored on the user's computer. The cookies are not secure. An

unauthorized user could copy a user's cookies to another computer system, and thereby gain access to the valuable information stored within the cookies.

Therefore a need exists for a data processing system and method for maintaining secure data blocks.

5

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210

SUMMARY OF THE INVENTION

5 A data processing system and method are disclosed for maintaining a secure data block within the system. A block of data is established within the system. The block of data is associated with a particular user and a particular application. A hardware master key pair is established for the system. The hardware master key pair includes a master private key and a master public key. The hardware master key pair is associated with the system for which it was established so that the master private key is known to only that system. The block of data is encrypted utilizing the master public key. The master private key is required to decrypt the encrypted block of data. This data processing system is the only system capable of decrypting the encrypted block of data.

10 The above as well as additional objectives, features, and advantages of the present invention will become apparent in the following detailed written description.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features are set forth in the appended claims. The present invention itself, however, as well as a preferred mode of use, further objectives, and advantages thereof, will best be understood by reference to the following detailed description of a preferred embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 illustrates a pictorial representation of a data processing system in accordance with the method and system of the present invention;

Figure 2 depicts a more detailed pictorial representation of the data processing system of **Figure 1** in accordance with the method and system of the present invention;

Figure 3 illustrates a high level flow chart which depicts establishing and storing a secure data block utilizing a hardware master key pair in a data processing system in accordance with the method and system of the present invention; and

Figure 4 depicts a high level flow chart which illustrates utilizing an encrypted data block to access an application associated with the data block in accordance with the method and system of the present invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

5 A preferred embodiment of the present invention and its advantages are better understood by referring to Figures 1-4 of the drawings, like numerals being used for like and corresponding parts of the accompanying drawings.

10 The present invention is a method and system for maintaining a secure data block within the system. A block of data is established within the system and is associated with a particular user and a particular application. The block of data includes information regarding the associated user and application. For example, the data block may include a user's name, password, and credit card number.

15 A hardware master key pair is established for the system. The hardware master key pair includes a master private key and a master public key. The hardware master key pair is associated with the system so that the master private key is known to only the data processing system for which it was established.

20 The data block is encrypted utilizing the master public key. The encrypted data block is stored in non-protected storage. The master private key is required to decrypt the encrypted block of data. Only this data processing system is capable of decrypting the encrypted block of data. If the encrypted data block is copied to another data
25 processing system, the data will be protected because the other data processing system will not have the first system's master private key, and will not be able to decrypt the encrypted data block.

30 When the data block is needed, such as by a browser program in order to access the associated application, the

decrypted data block is requested from the encryption device. The encrypted data block is then decrypted by the encryption device utilizing the hardware private key, which is stored in the encryption device.

5 **Figure 1** illustrates a pictorial representation of a data processing system including a plurality of client computer systems **104** coupled to a server computer system **100** utilizing a hub **102** in accordance with the method and system of the present invention. Each client computer system **104** and server computer system **100** may be implemented utilizing a computer system **30**. Server computer system **100** and client computer systems **104** are connected to hub **102** utilizing a communication link **106**. Communications link **106** may conform to a local area network standard such as the Ethernet specification, or may be a wide area network (WAN) utilizing a telephone network. Those skilled in the art will recognize that the invention described herein may be implemented utilizing any suitable type of data communications channel or link. In addition, communications link **106** may simultaneously include multiple different types of data communications channels.

10
15
20
25 Computer system **30** includes a computer **12**, a monitor **13**, a keyboard **14**, and a printer or plotter **15**. Computer system **30** may be implemented utilizing any commercially available computer system which has been suitably programmed and which has been modified as described below.

30 **Figure 2** depicts a more detailed pictorial representation of the data processing system of **Figure 1** in accordance with the method and system of the present invention. Computer **12** includes a planar (also commonly called a motherboard or system board) which is mounted within computer **12** and provides a means for mounting and

electrically interconnecting various components of computer 12 including a central processing unit (CPU) 200, system memory 206, and accessory cards or boards as is well known in the art.

5 CPU 200 is connected by address, control, and data busses 202 to a memory controller and peripheral component interconnect (PCI) bus bridge 204 which is coupled to system memory 206. An integrated drive electronics (IDE) device controller 220, and a PCI bus to Industry Standard
10 Architecture (ISA) bus bridge 204 are connected to PCI bus bridge 204 utilizing PCI bus 208. IDE controller 220 provides for the attachment of IDE compatible storage devices, such a removable hard disk drive 222. PCI/ISA
15 bridge 212 provides an interface between PCI bus 208 and an optional feature or expansion bus such as the ISA bus 214. PCI/ISA bridge 212 includes power management logic. PCI/ISA
20 bridge 212 is supplied power from battery 244 to prevent loss of configuration data stored in CMOS 213.

A PCI standard expansion bus with connector slots 210
25 is coupled to PCI bridge 204. PCI connector slots 210 may receive PCI bus compatible peripheral cards. An ISA standard expansion bus with connector slots 216 is connected to PCI/ISA bridge 212. ISA connector slots 216 may receive ISA compatible adapter cards (not shown). It will be
30 appreciated that other expansion bus types may be used to permit expansion of the system with added devices. It should also be appreciated that two expansion busses are not required to implement the present invention.

An I/O controller 218 is coupled to PCI-ISA bridge
35 controller 212. I/O controller 218 controls communication between PCI-ISA bridge controller 212 and devices and

peripherals such as floppy drive **224**, keyboard **14**, and mouse **228** so that these devices may communicate with CPU **200**.

PCI-ISA bridge controller **212** includes an interface for a flash memory **242** which includes an interface for address, data, flash chip select, and read/write. Flash memory **242** is an electrically erasable programmable read only memory (EEPROM) module and includes BIOS that is used to interface between the I/O devices and operating system.

Computer **12** includes a video controller **246** which may, for example, be plugged into one of PCI expansion slots **210**. Video controller **246** is connected to video memory **248**. The image in video memory **248** is read by controller **246** and displayed on monitor **13** which is connected to computer **12** through connector **250**.

Computer system **12** includes a power supply **240** which supplies full normal system power **243**, and has an auxiliary power main AUX **5 241** which supplies full time power to the power management logic **212**, and to a network adapter **230**.

Network adapter **230** includes a physical layer **234** and a media access controller (MAC) **232** coupled together utilizing a Media Independent Interface (MII) bus **252**. The MII bus **252** is a specification of signals and protocols which define the interfacing of a 10/100 Mbps Ethernet Media Access Controller (MAC) **232** to the underlying physical layer **234**. Network adapter **230** may be plugged into one of the PCI connector slots **210** (as illustrated) or one of the ISA connector slots **216** in order to permit computer system **30** to communicating with server **100** utilizing communications link **106**.

MAC 232 processes digital network signals, and serves as an interface between a shared data path, i.e. the MII bus 252, and the PCI bus 208. MAC 232 performs a number of functions in the transmission and reception of data packets. For example, during the transmission of data, MAC 232 assembles the data to be transmitted into a packet with address and error detection fields. Conversely, during the reception of a packet, MAC 232 disassembles the packet and performs address checking and error detection. In addition, MAC 232 typically performs encoding/decoding of digital signals transmitted over the shared path and performs preamble generation/removal, as well as bit transmission/reception. In a preferred embodiment, MAC 232 is an Intel 82557 chip. However, those skilled in the art will recognize that the functional blocks depicted in network adapter 230 may be manufactured utilizing a single piece of silicon.

Physical layer 234 conditions analog signals to go out to the network via an R45 connector 236. Physical layer 234 may be a fully integrated device supporting 10 and 100 Mbps CSMA/CD Ethernet applications. Physical layer 234 receives parallel data from the MII local bus 252 and converts it to serial data for transmission through connector 236 and over the network. Physical layer 234 is also responsible for wave shaping and provides analog voltages to the network. In a preferred embodiment, physical layer 234 is implemented utilizing an Integrated Services chip ICS-1890.

Physical layer 234 includes auto-negotiation logic that serves three primary purposes. First, it determines the capabilities of computer system 30. Second, it advertises its own capabilities to server computer 100. Third, it establishes a connection with server computer 100 using the highest performance connection technology.

In accordance with the present invention, the planar includes an encryption device **261** which includes an encryption/decryption engine **260** which includes an encryption/decryption algorithm which is utilized to encode and decode messages transmitted and received by the planar, and protected storage **262**. Engine **260** can preferably perform public/private key encryption. Engine **260** may access a protected storage device **262**. Protected storage device **262** is accessible only through engine **260**, and is a one-time writable device. Therefore, storage device **262** cannot be read or written to by the planar or any other device after the keys have programmed by system manufacturing or the system owner. Hardware master keys stored within storage **262** are protected by engine **260** and are not accessible to the planar or its components. Storage device **262** is utilized to store the hardware master key pair, including the master private key and master public key. Device **262** may be implemented utilizing an electronically erasable storage device, such as an EEPROM. Access may be gained to non-readable storage device **262** in order to initially store the master private key. However, after the master private key is stored, it cannot be read. The keys stored in EEPROM **262** may not be read by any component of the planar other than engine **260**.

Encryption device **261**, including engine **260** and EEPROM **262**, is coupled to PCI-ISA bridge **212** utilizing a system management (SM) bus **238**. System management bus **238** is a two-wire, low speed, serial bus used to interconnect management and monitoring devices. Those skilled in the art will recognize that encryption device **261** may be coupled to another bus within the planar.

Figure 3 illustrates a high level flow chart which depicts establishing and storing a secure data block

utilizing a hardware master key pair in a data processing system in accordance with the method and system of the present invention. The process starts as depicted at block 300 and thereafter passes to block 302 which illustrates establishing a hardware master key pair for data processing system 30. Next, block 304 depicts the storage of the master public key and master private key in protected storage 262 which is a one-time writable, protected storage in the encryption device. The process then passes to block 306 which illustrates an application executing on server computer system 100 establishing a data block which includes valuable information. The data block is associated both with a particular user and the application.

Next, block 308 depicts the encryption of the data block, including the valuable information, with the hardware master public key. Thereafter, block 310 illustrates the storage of the encrypted data block in storage within computer system 30 such as hard drive 222. The process then terminates as illustrated at block 312.

Figure 4 depicts a high level flow chart which illustrates utilizing an encrypted data block to access an application associated with the data block in accordance with the method and system of the present invention. The process starts as illustrated at block 400 and thereafter passes to block 402 which depicts a browser initiating a session with an application or site. Thereafter, block 406 depicts the browser identifying the data block associated with the user and the selected application, and requesting the data block from the encryption device.

Next, block 408 illustrates the identified, encrypted data block being copied from storage into the encryption device. Thereafter, block 410 depicts the encryption device

decrypting the data block utilizing the hardware private key. The process then passes to block 412 which illustrates the encryption device sending the decrypted data block to the browser. Next, block 414 depicts the browser sending the decrypted data block or components of the decrypted data block to the application. The process then terminates as illustrated at block 416.

While a preferred embodiment has been particularly shown and described, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the present invention.

CLAIMS:

1. A method in a data processing system for maintaining a secure data block within said system, said method comprising the steps of:

5 establishing a block of data within said system, said block of data being associated with a particular user and a particular application;

10 establishing a hardware master key pair for said system, said hardware master key pair including a master private key and a master public key, said hardware master key pair being associated with said system so that said master private key is known to only said system; and

15 encrypting said block of data utilizing said master public key, said master private key being required to decrypt said encrypted block of data, wherein only said data processing system is capable of decrypting said encrypted block of data.

20 2. The method according to claim 1, further comprising the step of storing said encrypted block of data in a non-protected storage device.

3. The method according to claim 2, further comprising the steps of:

25 establishing an encryption device having an encryption engine and a protected storage device, said protected storage device being accessible only through said encryption engine; and

storing said hardware master key pair in said protected storage device.

4. The method according to claim 3, further comprising the step of said encryption engine encrypting said block of data utilizing said master public key stored in said protected storage device.

5. The method according to claim 4, further comprising the step of a remote data processing system executing said application.

6. The method according to claim 5, further comprising the step of establishing a browser program for accessing said application.

7. The method according to claim 6, further comprising the steps of:

said browser program initiating a session with said application;

said browser requesting said encryption device to decrypt said encrypted block of data;

in response to said request, said encryption device decrypting said encrypted block of data utilizing said master private key; and

said encryption device transmitting said decrypted block of data to said browser program.

8. The method according to claim 7, further comprising the step of said browser program transmitting said decrypted block of data to said application.

9. The method according to claim 8, wherein said step of storing said encrypted block of data in said non-protected storage further comprises the step of storing said encrypted block of data in a hard drive.

5 10. A data processing system for maintaining a secure data block within said system, comprising:

said system executing code for establishing a block of data within said system, said block of data being associated with a particular user and a particular application;

10 said system executing code for establishing a hardware master key pair for said system, said hardware master key pair including a master private key and a master public key, said hardware master key pair being associated with said system so that said master private key is known to only said system; and

15 said system executing code for encrypting said block of data utilizing said master public key, said master private key being required to decrypt said encrypted block of data, wherein only said data processing system is capable of
20 decrypting said encrypted block of data.

11. The system according to claim 10, further comprising said system executing code for storing said encrypted block of data in a non-protected storage device.

12. The system according to claim 11, further comprising:

25 an encryption device having an encryption engine and a protected storage device, said protected storage device being accessible only through said encryption engine; and

said encryption device executing code for storing said hardware master key pair in said protected storage device.

13. The system according to claim 12, further comprising said encryption engine executing code for encrypting said block of data utilizing said master public key stored in said protected storage device.

14. The system according to claim 13, further comprising a remote data processing system capable of executing said application.

15. The system according to claim 14, further comprising said system executing code for establishing a browser program for accessing said application.

16. The system according to claim 15, further comprising:

said system executing code for said browser program initiating a session with said application;

said system executing code for said browser requesting said encryption device to decrypt said encrypted block of data;

in response to said request, said encryption device capable of decrypting said encrypted block of data utilizing said master private key; and

said encryption device executing code for transmitting said decrypted block of data to said browser program.

17. The system according to claim 16, further comprising said system executing code for said browser program

transmitting said decrypted block of data to said application.

18. The system according to claim 17, further comprising a hard drive for storing said encrypted block of data.

5 19. A data processing system for maintaining a secure data block within said system, comprising:

said system executing code for establishing a block of data within said system, said block of data being associated with a particular user and a particular application;

10 an encryption device executing code for establishing a hardware master key pair for said system, said hardware master key pair including a master private key and a master public key, said hardware master key pair being associated with said system so that said master private key is known to only said system;

15 said system executing code for encrypting said block of data utilizing said master public key, said master private key being required to decrypt said encrypted block of data, wherein only said data processing system is capable of
20 decrypting said encrypted block of data;

said system executing code for storing said encrypted block of data in a hard drive;

25 said encryption device having an encryption engine and a protected storage device, said protected storage device being accessible only through said encryption engine;

said encryption device executing code for storing said hardware master key pair in said protected storage device;

said encryption engine executing code for encrypting said block of data utilizing said master public key stored in said protected storage device;

a remote data processing system capable of executing said application;

said system executing code for establishing a browser program for accessing said application;

said system executing code for said browser program initiating a session with said application;

said system executing code for said browser requesting said encryption device to decrypt said encrypted block of data;

in response to said request, said encryption device capable of decrypting said encrypted block of data utilizing said master private key;

said encryption device executing code for transmitting said decrypted block of data to said browser program;

said system executing code for said browser program transmitting said decrypted block of data to said application.

ABSTRACT OF THE DISCLOSURE

DATA PROCESSING SYSTEM AND METHOD FOR MAINTAINING SECURE
DATA BLOCKS

5 A data processing system and method are disclosed for
maintaining a secure data block within the system. A block of
data is established within the system. The block of data is
associated with a particular user and a particular
application. A hardware master key pair is established for
the system. The hardware master key pair includes a master
private key and a master public key. The hardware master key
pair is associated with the system for which it was
established so that the master private key is known to only
that system. The block of data is encrypted utilizing the
master public key. The master private key is required to
decrypt the encrypted block of data. This data processing
system is the only system capable of decrypting the encrypted
block of data.

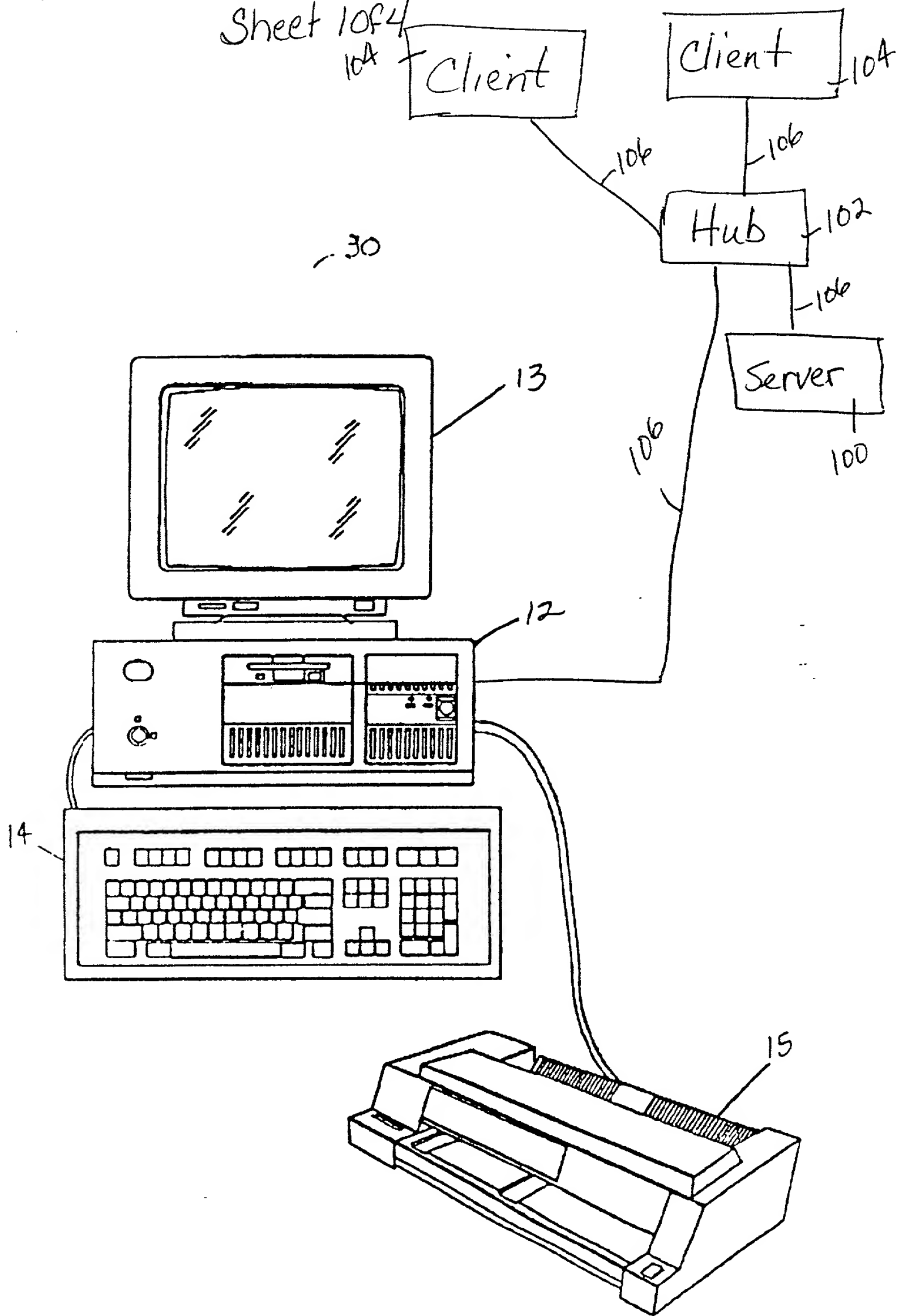


Fig. 1

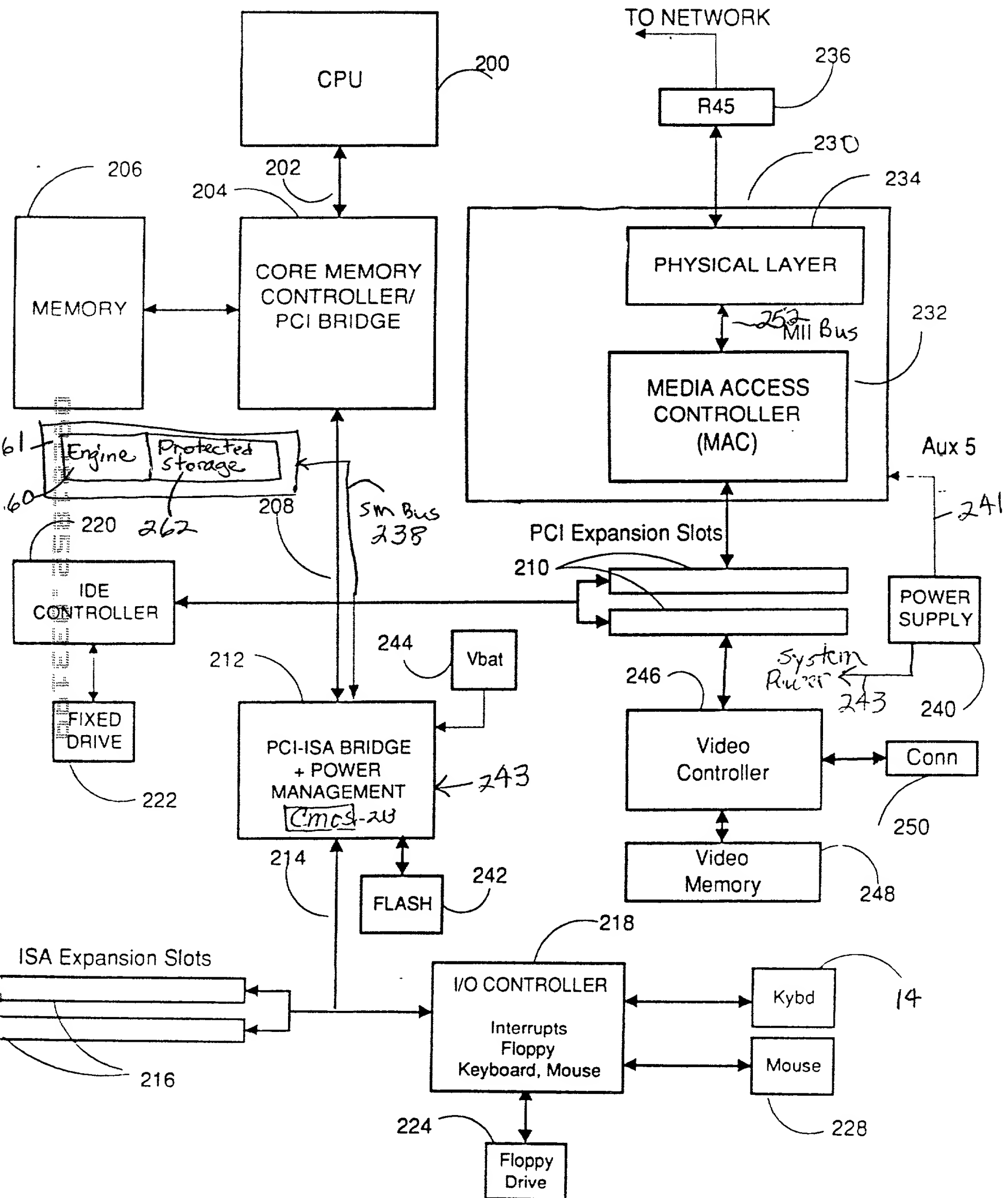


Fig. 2

RP999048

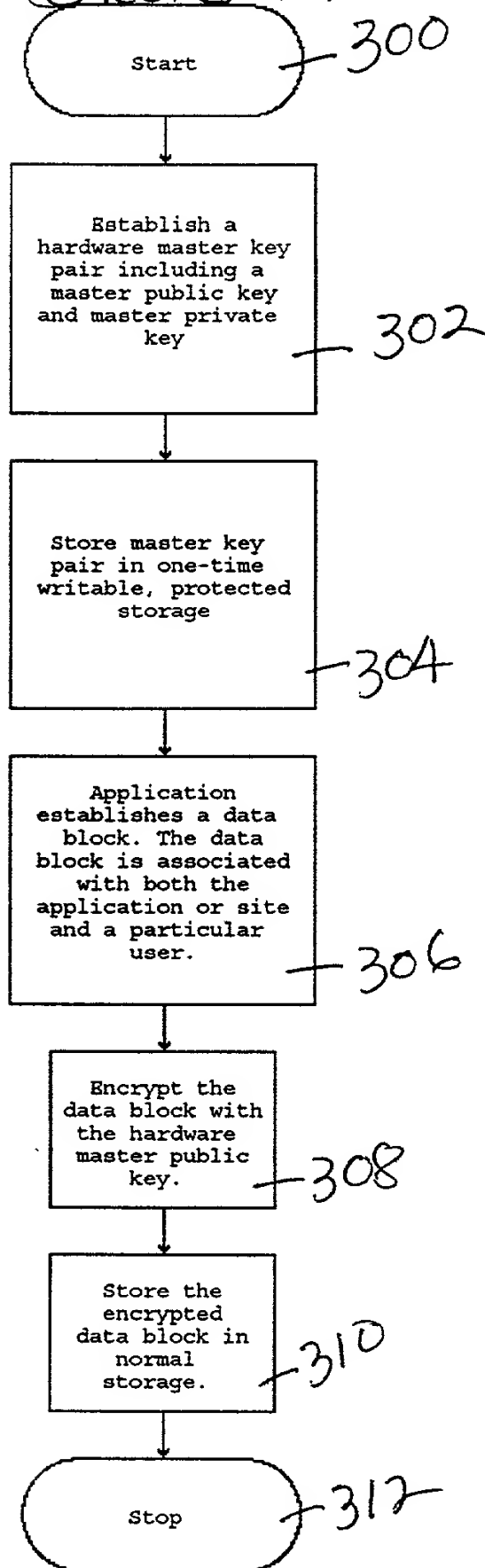


Fig. 3

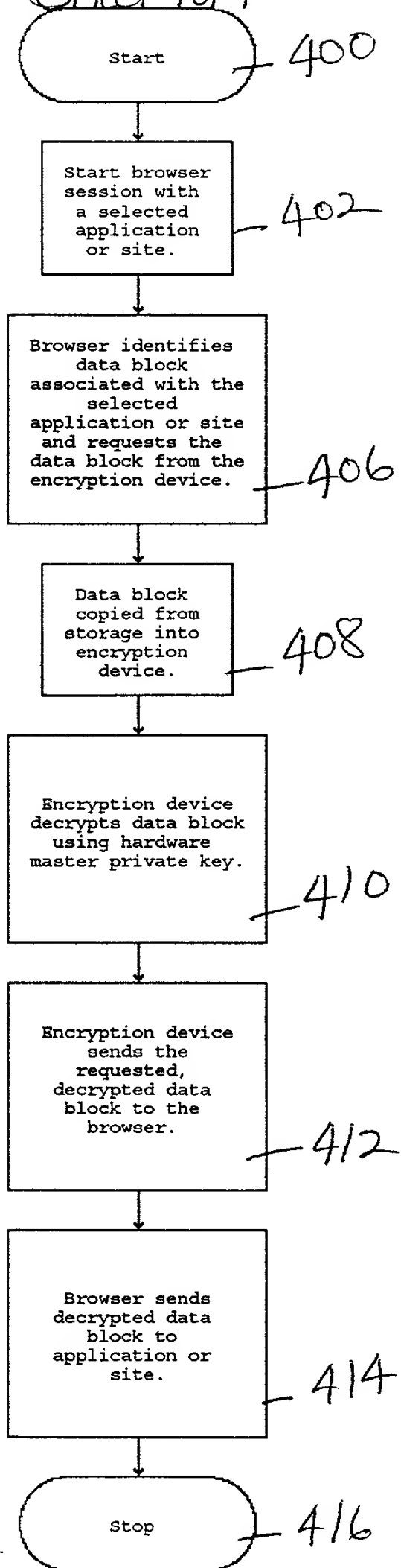


Fig. 4

**DECLARATION AND POWER OF ATTORNEY FOR
PATENT APPLICATION**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

DATA PROCESSING SYSTEM AND METHOD FOR MAINTAINING SECURE DATA BLOCKS

the specification of which (check one)

X is attached hereto.

— was filed on _____
as Application Serial No. _____
and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):	Priority Claimed
<div style="display: flex; justify-content: space-between;"> <div>_____ (Number)</div> <div>_____ (Country)</div> <div>_____ (Day/Month/Year)</div> </div>	<div style="display: flex; justify-content: flex-end;"> <div>____ Yes ____ No</div> </div>

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

_____ (Application Serial #)	_____ (Filing Date)	_____ (Status)
---------------------------------	------------------------	-------------------

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both,

under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Horace St. Julian, Reg. No. 30,329; Bernard D. Bogdon, Reg. No. 27,773; George E. Grosser, Reg. No. 25,629; Anthony N. Magistrale, Reg. No. 35,595; Daniel E. McConnell, Reg. No. 20,360; Martin J. McKinley, Reg. No. 31,782; Christopher A. Hughes, Reg. No. 26,914; Edward A. Pennington, Reg. No. 32,588; John E. Hoel, Reg. No. 26,279; Joseph C. Redmond, Jr., Reg. No. 18,753; Max Ciccarella, Reg. No. 39,454; Andrew J. Dillon, Reg. No. 29,634; Justin M. Dillon, Reg. No. 42,486; John G. Graham, Reg. No. 19,563; Kenneth C. Hill, Reg. No. 29,650; Melvin A. Hunn, Reg. No. 32,574; Jack V. Musgrove, Reg. No. 31,986; Antony P. Ng, Reg. No. 43,032; Brian F. Russell, Reg. No. 40,796; and Daniel E. Venglarik, Reg. No. 39,409.

Send correspondence to: Andrew J. Dillon, FELSMAN, BRADLEY, VADEN, GUNTER & DILLON, LLP, Suite 350, Lakewood on the Park, 7600B North Capital of Texas Highway, Austin, Texas 78731, and direct all telephone calls to Andrew J. Dillon, (512) 343-6116.

FULL NAME OF SOLE OR FIRST INVENTOR: Daryl Carvis Cromer

INVENTORS SIGNATURE: Daryl Carvis Cromer DATE: 3/30/99

RESIDENCE: 2631 Grande Valley Circle Drive
Cary, North Carolina 27513

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 2631 Grande Valley Circle Drive
Cary, North Carolina 27513

FULL NAME OF SECOND INVENTOR: Howard Locker

INVENTORS SIGNATURE: Howard Locker DATE: 3/31/99

RESIDENCE: 103 Paladin Place
Cary, North Carolina 27513

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 103 Paladin Place
Cary, North Carolina 27513

FULL NAME OF THIRD INVENTOR: Andy Lloyd Trotter

INVENTORS SIGNATURE: Andy Lloyd Trotter DATE: 03/30/99

RESIDENCE: 8203-107 Green Lantern St.
Raleigh, North Carolina 27613

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 8203-107 Green Lantern
Raleigh, North Carolina 27613

DOCKET NUMBER: RP9-99-048

FULL NAME OF FOURTH INVENTOR: James Peter Ward

INVENTORS SIGNATURE: James Peter Ward DATE: 3/31/99

RESIDENCE: 107 Hemingway Forest Place
Raleigh, North Carolina 27607

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 107 Hemingway Forest Place
Raleigh, North Carolina 27607